IN THE SPECIFICATION:

Please amend the paragraphs in the published application as follows:

[0007] FIG. 2 shows how the user connects the ISP 203 via a PSTN (Public Switched Telephone Network) 202 of a communication enterprise from his/her home 201, thereby beginning communication on the Internet. The PC [[111]] 211 installed at the user home 201 is connected to a modem 212 used to modulate/demodulate communication signals. A RAS (Remote Authentication Server) 231, an authentication server 232, and a NAT (Network Address Translator) 233 are installed in the ISP 203.

[0032] FIG. 3 shows a block diagram of a method for providing data communication services in an embodiment of the present invention. In FIG. 3, a user home 301 connects a local switching center 303 via a PSTN 302. A PC 311 installed at the user home 301 connects a modem 312, thereby communicating with a local access server (AS) 331 provided in the local switching center 303. The local switching center 303 is connected to an ISP-A 305 and an ISP-B 306 that are ISPs via an IP network 304. The ISP-A 305 and the ISP-B 306 are connected to the Internet 307 so that they can provide the user with an Internet connection service. In the IP network 304, an address translation gateway (AT-GW) 341 used to translate a private address assigned to the user to an IP address assigned from an ISP, a local DNS server 342 used to accept name solution queries from users, a portal server 343 that is a web server used to display information required when the user selects an ISP; a local service server 344 used by the communication enterprise to provide its users with contents inside its own network not via the Internet; and a user management server 345 used to hold ISP contract information of each user are installed. Each of the servers are connected to the local switching center 303 via a router 346. A private address is assigned to an interface used to connect each of the servers to a router 346. The AT-GW 341, the local DNS 342, and the portal server 343 are connected to the ISP-A 305 and the ISP-B 306 respectively via a router 347 that uses an interface that is different from the private address assigned one. A global address is assigned to this interface connected to the router 347.

[0036] The AT-GW 341 holds an address translation table used to translate addresses. FIG. 5 shows an example of the address translation table used when the PC 311 connects this system. This address translation table includes items of user ID 501; private address 502; global address 503; arrival time of last packet 504, etc. In this example, a user whose ID is

XXX is connected to a user whose ID is YYY. In the first record, a user ID "XXX" 511, a private address "a.b.c.d" [[512]] 521, a global address "null" 531, and an arrival time of last packet "null" 541 are registered respectively. Because "null" is registered in both of the global address and arrival time of last packet fields, the user whose ID is "XXX" is not connected to any ISP yet. The table items to be registered after the user is connected to an ISP will be described later. In the same way, in the second record, a user ID "YYY" 512, a private address "a.b.c.e" 522, a global address "null" 532, and an arrival time of last packet "null" 542 are registered respectively.

[0039] FIG. 8 shows a user information contract table registered in the user management server 345. The items registered in this table are user ID 801; contract ISP 802; contract information 803, etc. In this example, three items are registered in the table. The first record contains a user ID "XXX" in a field 811, which is "XXX811", a contract ISP, which is ISP-A 821, and contract information, which is ISP user ID="abc" and an ISP password="def" in this example. Those information items are sent back to the AT-GW 341 as a user information response (step 704). Sometimes, the same user has plural records in the table. The second and third records are such an example. In those records, "YYY" is registered in both fields 812 and 813 as a user ID and "ISP-A" [[922]] and "ISP-B" in the fields 821, 822, 823 [[922]] are registered as contract ISPs. In the field [[932]] 832, ISP user ID="ghi"; ISP password="jkl" are registered as the information of the user's (user ID: YYY) contract with the ISP-A. In the field [[933]] 833, ISP user ID="mno"; ISP password="pqr" is registered as the information of user's (user ID: YYY) contract with the ISP-B.

[0040] Knowing that the user has a contracted ISP from those information items (step 705), the AT-GW 341 sends contract information such as the ISP user ID, the ISP password, etc. to the ISP authentication server 361 and requests the server 361 to authenticate the user by using such a protocol as the RADUS (Remote Authentication Dial-In User Service) or the like (step 706). When the authentication is completed correctly, the authentication server 361 assigns a global address and reports it to the AT-GW 341 (step 707) . The AT-GW 341 then registers the assigned global address in the address translation table (step 708) . This completes the connection to the ISP.

[0042] FIG. 9 shows how the processings are done with respect to the address translation table. In FIG. 9, the state of the table shown in FIG. 5 is changed as follows. The global

address, which has been a null 531, is changed to "f.g.h.i" [[831]] 931 and the arrival time of last packet, which has been a null 541, is changed to, for example, 10:5:15 841, which denotes an address translation time respectively in the record of the user whose ID: XXX. The example denotes that the user's connection to the ISP is completed, since a global address and an arrival time of the last packet are registered such way.

[0043] FIG. 10 shows a communication sequence to be performed when the user does not contract with any ISP. At first, the PC 311 sends a packet to the Internet via the AS 331 (step 1001). Because the destination address of the packet is a global address at this time, the packet arrives in the AT-GW 341. The AT-GW 341 then searches in the address translation table by using the source address as a key as described above (step 1002) and finds that no global address is registered in the table. Thus, the AT-GW 341 sends the user ID and issues a user information request to the user management server 345 (step 1003). Then, a user information response (step 1004) is sent back to the user management server 345. However, because the user does not contract with any ISP, the AT-GE 341 finds the fact from the response (step 1005). The AT-GW 345 knows that the received packet is discarded (step 1006) and the PC 311 cannot connect an ISP due to a connection timeout, since there is no ISP contracted by the user.

[0044] FIG. 11 shows a sequence of communication between the user and the portal server 343. The PC 311 specifies a contract screen URL (Uniform Resource Location) to the portal server 343 and issues a contract screen request with use of the HTTP (Hyper Text Transfer Protocol) (step 1101). Then, the portal server 343 starts up the GCI (Common Gateway Interface) and a JAVA servelet to execute the following operations. At first, the portal server extracts the network address of the PC 311 from the received packet and sends the address to the AT-GW 341 to request the user ID (step 1102). The AT-GW 341 searches the user ID by using the received address as a key and sends the found user ID and connection information that denotes presence of a connection to an ISP to the portal server 343 (step 1103). Receiving the user ID, the portal server 343 sends the user ID to the user management server 345 to request information of contract ISP (step 1104). The user management server 345 then checks each record in the user contract information table shown in FIG. 8 by using the user ID as a key and sends the contract ISP and the contract information to the portal server 343 (step 1105). The portal server 343 generates a web page according to those information items and sends the screen as shown in FIG. 12 to the PC 311 (step 1106).

[0047] FIG. 13 shows a sequence for automatical disconnection of an ISP. The AT-GW 341 keeps the operation of a process that monitors the address translation table. In this process, a timer is set at first (step 1301). When a set time is reached, a timer interruption (step 1302) starts up the process. Then, in step 1303, the process compares the arrival time of the last packet shown in step 941 in FIG. 9 with the current time. When there is any record still existing in a certain time after the user sends the last packet, the process disconnects the ISP described in the record with use of the RADIUS protocol (step 1304). After that, the process returns to the processing in step 1301 (step 1305). Consequently, the ISP is disconnected automatically in a certain time after the communication stops whether it is requested or not.